

Privacy notice and choice

Lorrie Faith Cranor

September 23, 2014

8-533 / 8-733 / 19-608 / 95-818:
Privacy Policy, Law, and Technology

Carnegie
Mellon
University

CyLab



Engineering &
Public Policy



Summary and highlight example

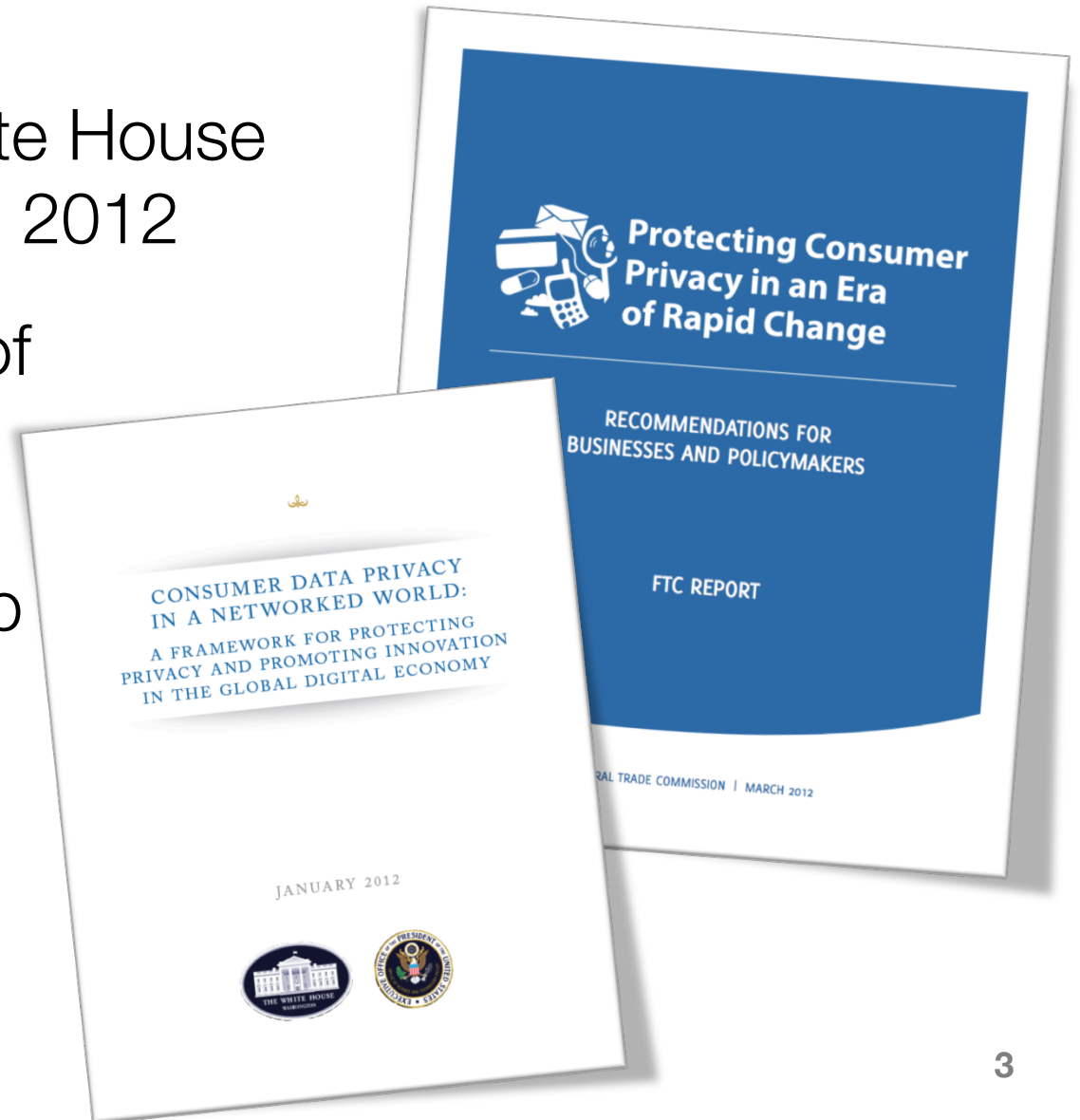
Question 1:

Brandimarte – Summary: The experiments described in this paper tested personal privacy attitudes in relation to the amount of control over the personal information being revealed. By varying control over information release in three separate studies, the experiments revealed a paradoxical effect such that increased control over the release of information increased willingness to share sensitive information, independent of how accessible the information is to others. This result raises the concern that technologies that give users greater control over the release of their information may actually expose them to greater risk if they lead to users being more willing to disclose information [1].

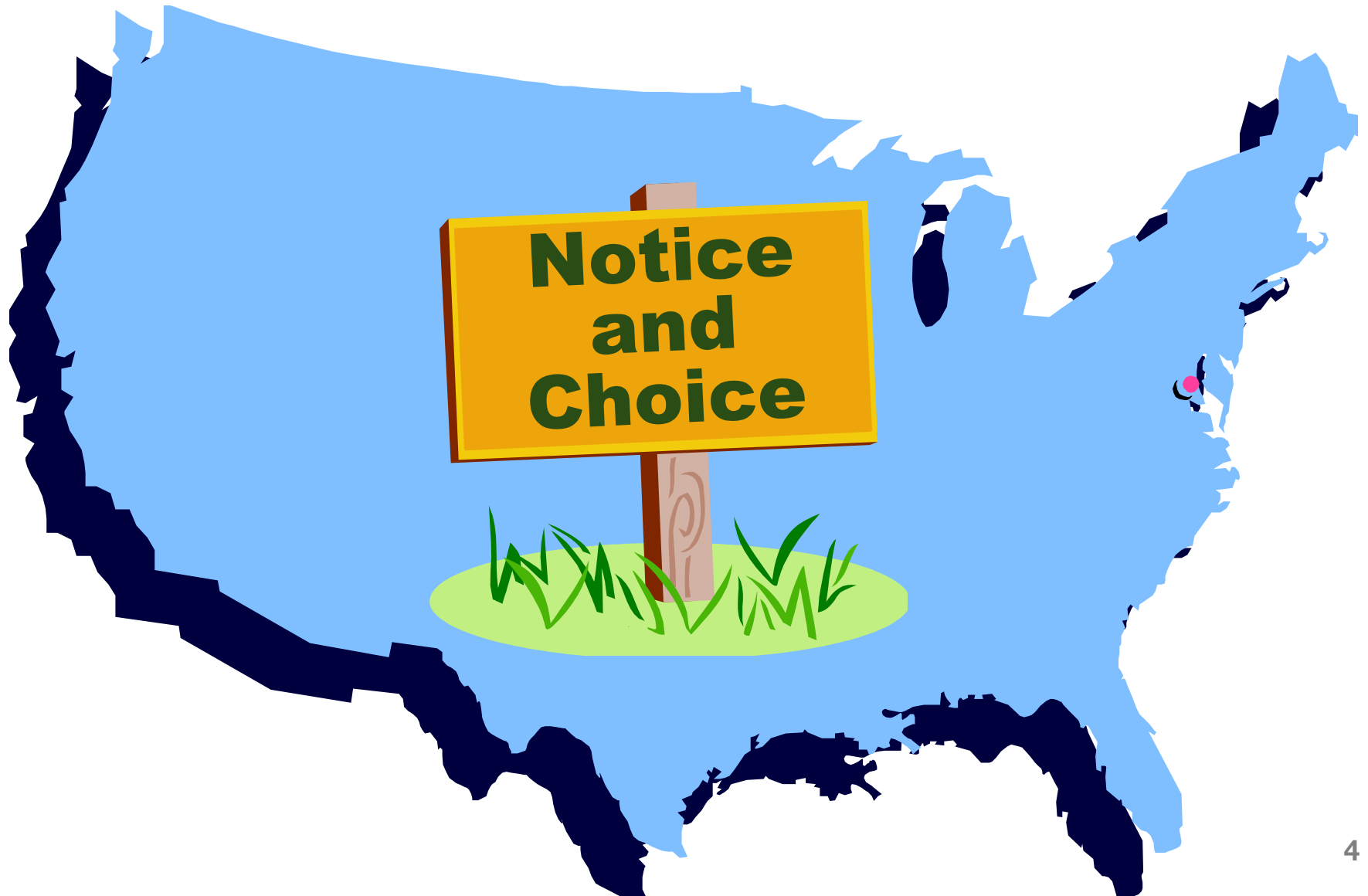
Brandimarte – Highlight: It is very interesting to me that perceived control over the dissemination of personal information has a greater effect on people's willingness to disclose information than the objective risk of the disclosure. Though all three experiments supported this conclusion, I think it was best reflected in Study 1, where students who were told their profiles would definitely be published online answered intrusive questions at a greater rate than students who were told that 50% of the profiles would be published at random. Even though the first set of students had a 100% chance of disclosure and the second set 50%, the perceived lack of control in the publication of the information seems to have had an influence on the privacy attitudes of those students [1].

US government privacy reports

- U.S. FTC and White House reports released in 2012
- U.S. Department of Commerce multi-stakeholder process to develop enforceable codes of conduct



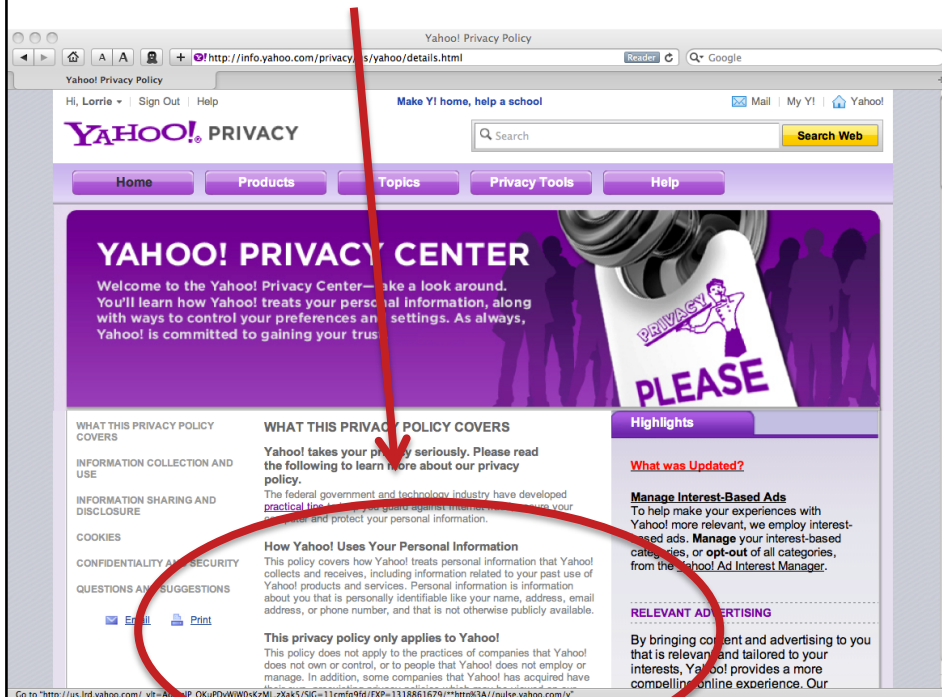
Privacy self regulation



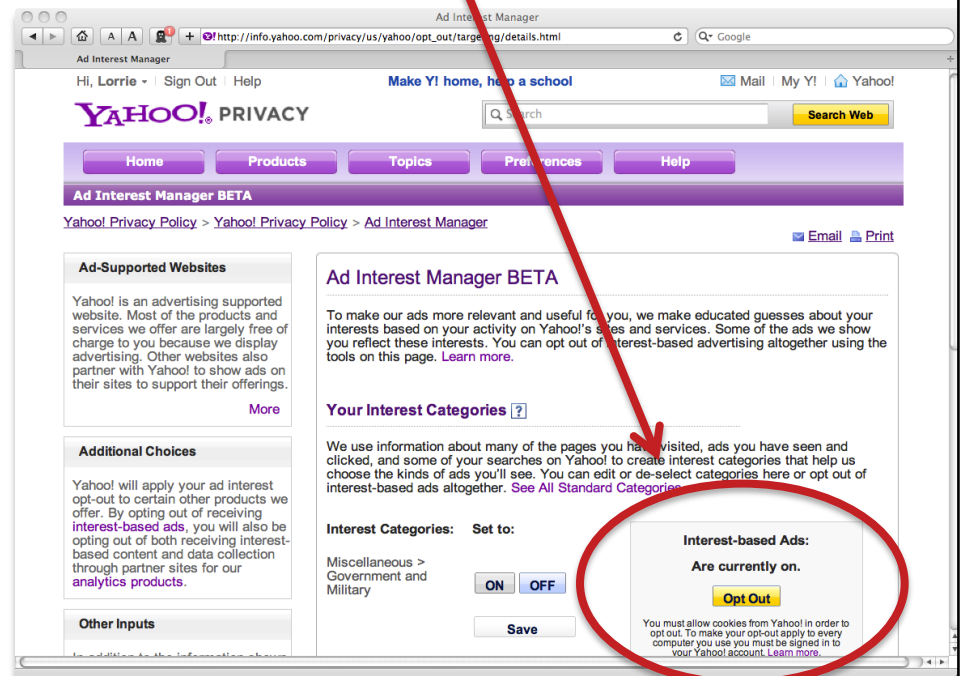
Notice and choice

Protect privacy by giving people control over their information

Notice about data collection and use



Choices about allowing their data to be collected and used in that way



[illegible][illegible][illegible][illegible]

A series of horizontal bars of varying lengths and shades of gray, representing a data visualization. The bars are arranged in a vertical stack, with some being solid black and others being light gray. The lengths of the bars vary, with some being the full width of the image and others being shorter. The bars are arranged in a vertical stack, with some being solid black and others being light gray. The lengths of the bars vary, with some being the full width of the image and others being shorter.

“In theory there is no
difference between theory and
practice. In practice there is.”

—Yogi Berra

How effective is privacy
notice and choice **in practice**?

[Français](#)[Home](#)[Contact Us](#)[Help](#)[Search](#)[canada.gc.ca](#)[Home](#) ► [News Room](#)

Search

[Search](#)

Advanced search

Sections

[About Us](#)[Legal Corner](#)[Commissioner's Findings](#)[Parliamentary Activities](#)[Resources](#)[News Room](#)[Frequently Asked Questions](#)[A-Z Index](#)

Transparency

[Completed Access to Information Requests](#)[Proactive Disclosure](#)

HOW TO FILE

[A privacy complaint](#)

SECURING PERSONAL INFORMATION

News

Global Privacy Enforcement Network Internet Privacy Sweep Questions and Answers

May 6, 2013

What will happen during the Internet Privacy Sweep? What is the goal?

Privacy enforcement authorities participating in the Sweep will designate individuals within their organizations to search the Internet in a coordinated effort to assess privacy practices related to a predetermined theme – this year the theme is Privacy Practice Transparency.

The Sweep will provide flexibility for privacy enforcement authorities to tailor their search within this common theme to focus on issues that are relevant in the context of domestic legislation, market factors and strategic priorities.

The purpose of the Sweep is *not* to conduct an in-depth analysis of the privacy practice transparency of each website, but to replicate the consumer experience by spending a few minutes per site checking for performance against set common indicators.

The Sweep is not an investigation, nor is it intended to conclusively identify

News

Year [View](#)

Speeches

Year [View](#)

UPCOMING EVENTS

GO

Media Relations

Contact:

[Anne-Marie Hayden](#)

Non-journalists are invited to contact our Information Centre. Please call 1-800-282-1376 (toll free) or (613) 947-1698 and ask to speak with an Information Officer.

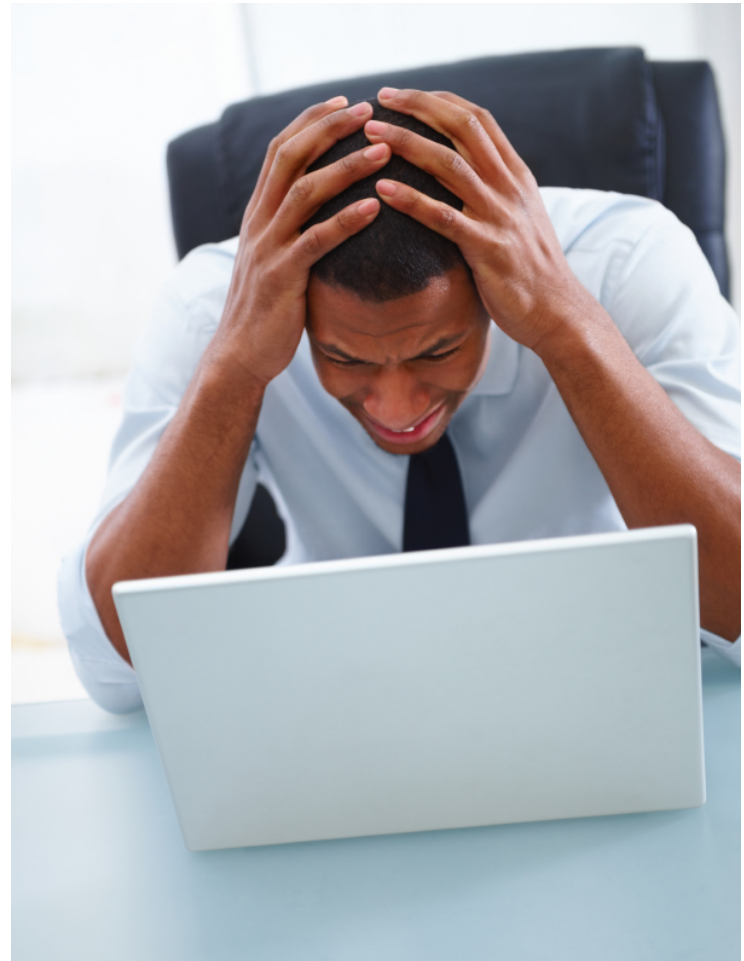
Address:

112 Kent Street
Ottawa, ON
K1A 1H3
Fax: (613) 995-1139

Nobody wants to read privacy policies

“the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand”

- *Protecting Consumer Privacy in an Era of Rapid Change*. Preliminary FTC Staff Report. December 2010.



Cost of reading privacy policies

- What would happen if everyone read the privacy policy for each site they visited once each month?
- Time = 244/hours year
- Cost = \$3,534/year
- National opportunity cost for time to read policies: \$781 billion



A. McDonald and L. Cranor. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society. 2008 Privacy Year in Review Issue. <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>



Your Data is Used Only for the Intended Use



Your Data May be Used for Purposes You Do Not Intend



Your data is never given to advertisers.



Site gives your data to advertisers.



Your data is never bartered or sold.



Your data may be bartered or sold.



Data is given to law enforcement only when legal process is followed.



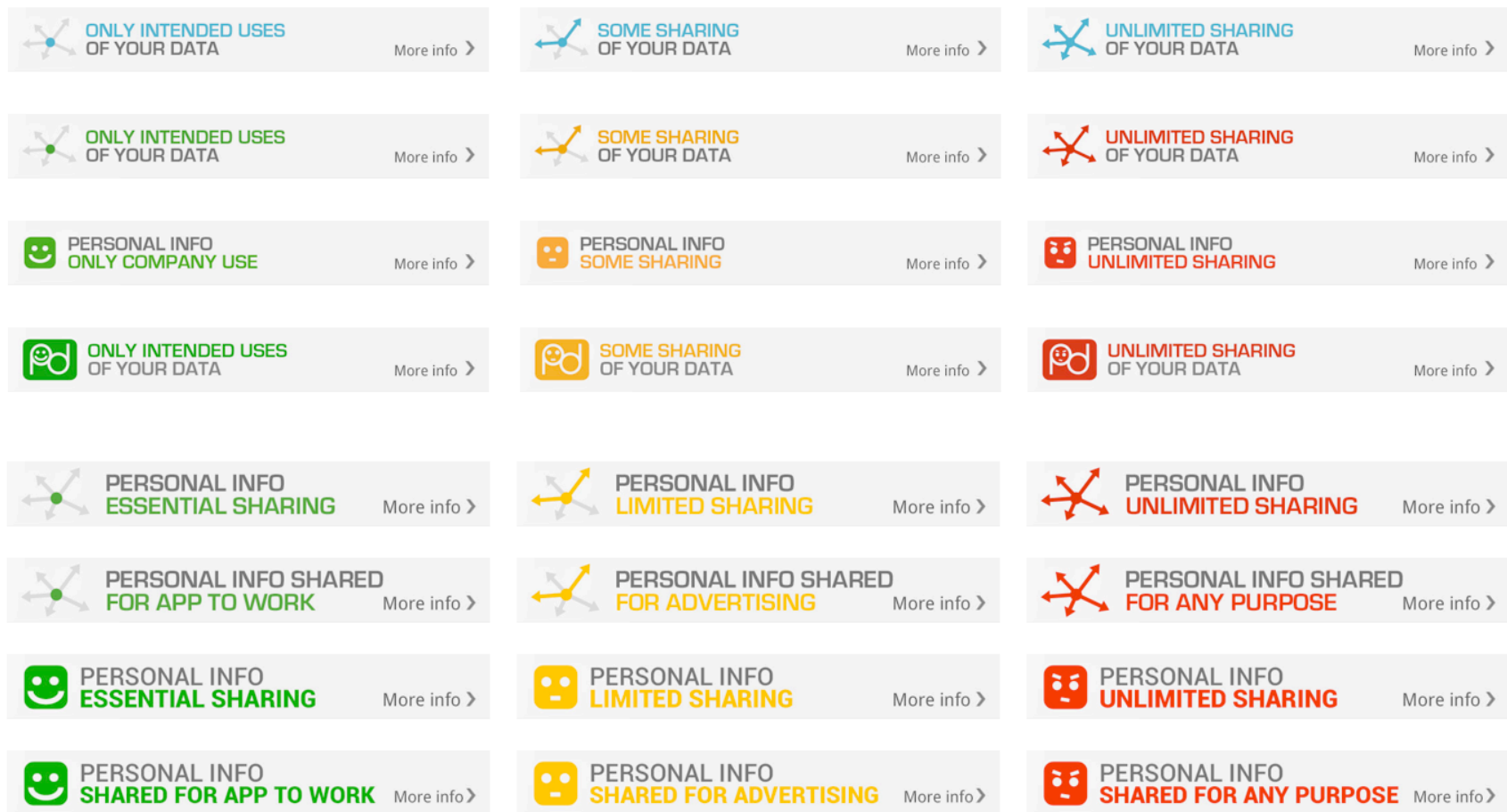
Data may be given to law enforcement even when legal process is not followed.



Your data is kept for less than 1 month.



Your data may be kept indefinitely.



Smartphone App Privacy Icon Study Conducted for
LifeLock, Inc. by Cranor et al., 2013

Towards a privacy “nutrition label”

- Standardized format
 - People learn where to find answers
 - Facilitates policy comparisons
- Standardized language
 - People learn terminology
- Brief
 - People find info quickly
- Linked to extended view
 - Get more details if needed



Iterative design process

- Series of studies
 - Focus groups
 - Lab studies
 - Online studies
- Metrics
 - Reading-comprehension (accuracy)
 - Time to find information
 - Ease of policy comparison
 - Subjective opinions, ease, fun, trust

P.G. Kelley, J. Bresee, L.F. Cranor, and R.W. Reeder.
A “Nutrition Label” for Privacy. SOUPS 2009.

P.G. Kelley, L.J. Cesca, J. Bresee, and L.F. Cranor.
Standardizing Privacy Notices: An Online Study
of the Nutrition Label Approach. CHI2010.

Acme						
information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
financial information						
health information						
preferences		opt out	opt out			
purchasing information		opt out	opt out			
social security number & gov't ID						
your activity on this site		opt out	opt out			
your location						

Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

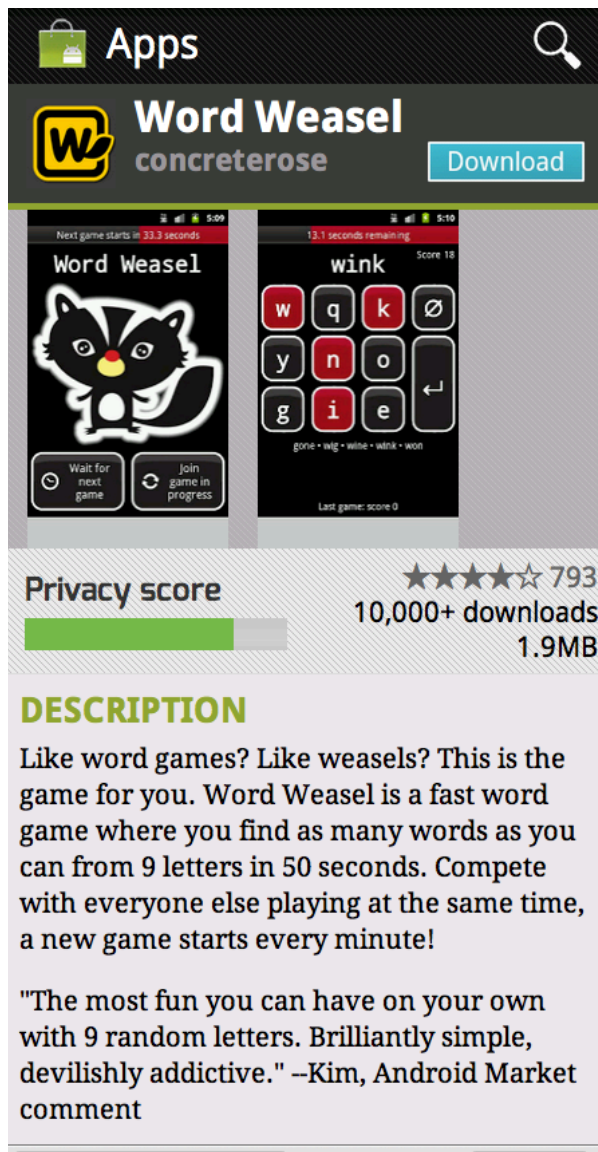
we will collect and use your information in this way

by default, we will collect and use your information in this way unless you tell us not to by opting out

we will not collect and use your information in this way

by default, we will not collect and use your information in this way unless you allow us to by opting in

Privacy label for Android



Word Weasel
concreterose [Download](#)

Next game starts in 33.3 seconds

Word Weasel

Wait for next game

Join game in progress

wink

Score 18

gone • wig • wise • wink • won

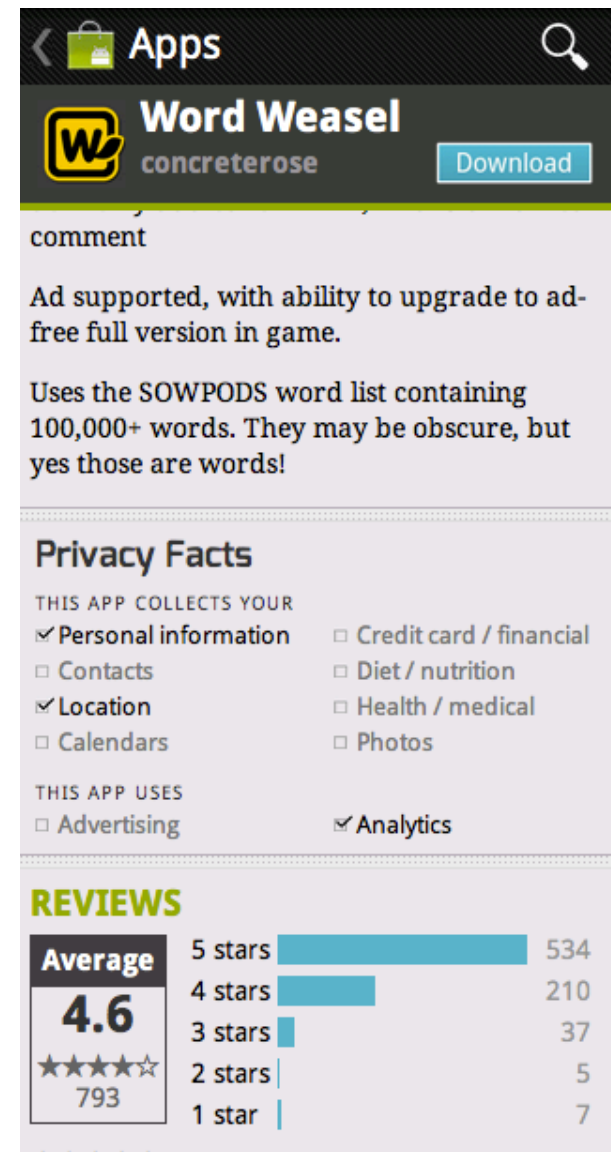
Last game: score 0

Privacy score ★★★★★ 793
10,000+ downloads
1.9MB

DESCRIPTION

Like word games? Like weasels? This is the game for you. Word Weasel is a fast word game where you find as many words as you can from 9 letters in 50 seconds. Compete with everyone else playing at the same time, a new game starts every minute!

"The most fun you can have on your own with 9 random letters. Brilliantly simple, devilishly addictive." –Kim, Android Market comment



Word Weasel
concreterose [Download](#)

comment

Ad supported, with ability to upgrade to ad-free full version in game.

Uses the SOWPODS word list containing 100,000+ words. They may be obscure, but yes those are words!

Privacy Facts

THIS APP COLLECTS YOUR

- ☒ Personal information
- ☐ Contacts
- ☒ Location
- ☐ Calendars
- ☐ Credit card / financial
- ☐ Diet / nutrition
- ☐ Health / medical
- ☐ Photos

THIS APP USES

- ☐ Advertising
- ☒ Analytics

REVIEWS

Average 4.6 ★★★★★ 793

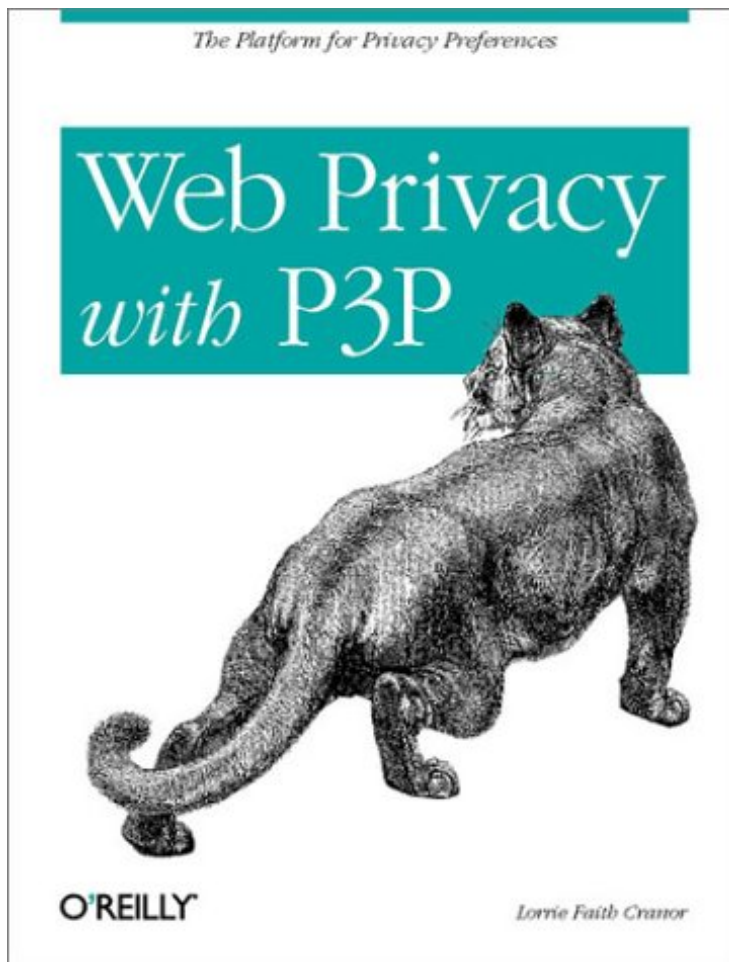
Stars	Count
5 stars	534
4 stars	210
3 stars	37
2 stars	5
1 star	7

Role play studies

- Task for participants in lab or online
 - Select apps for friend with new Android phone
 - Choose from 2 similar apps w/ different permission requests in each of 6 categories
 - Click on app name to visit download screens
- Post-task questionnaire
- Participants who saw Privacy Facts more likely to select apps that requested fewer permissions
 - Other factors such as brand and rating reduce effect

P.G. Kelley, L.F. Cranor, and N. Sadeh. Privacy as part of the app decision-making process. CHI 2013.

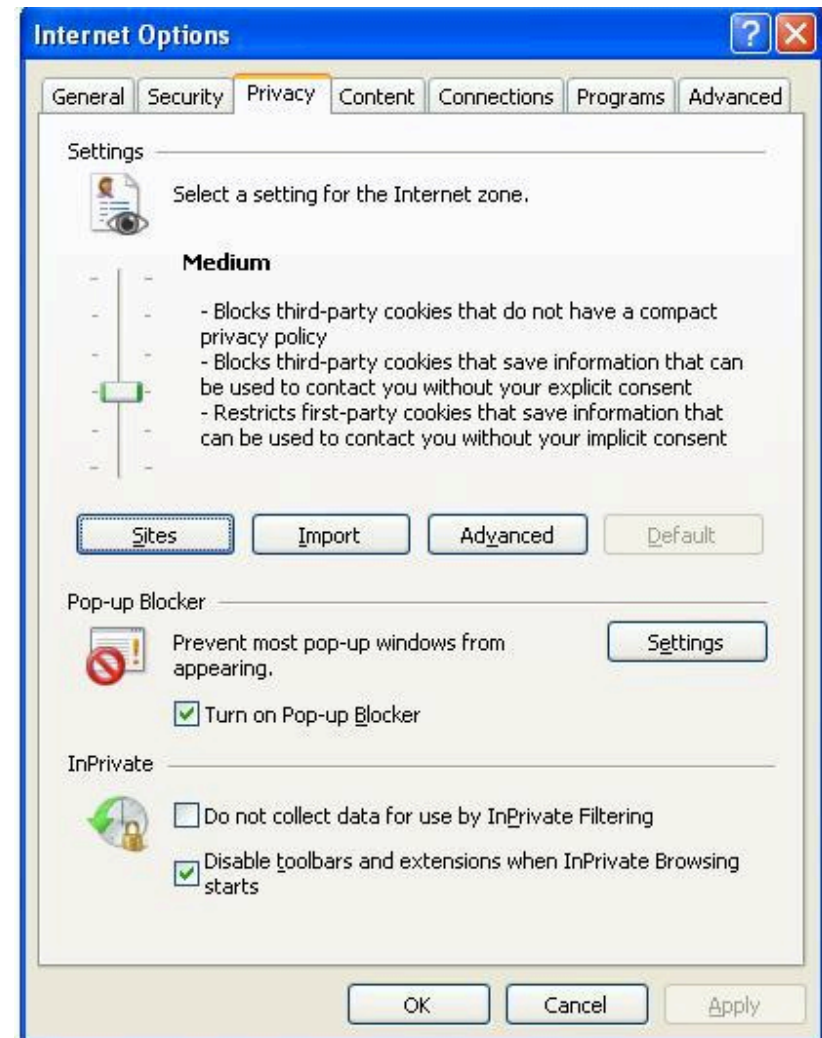
Let your computer read for you



- Platform for Privacy Preferences (P3P)
- W3C specification for XML privacy policies
 - Proposed 1996
 - Adopted 2002
- Optional P3P compact policy HTTP headers to accompany cookies
- Lacks incentives for adoption

P3P in Internet Explorer

- P3P implemented in IE 6, 7, 8, 9, 10 ...
- Default privacy setting
 - Rejects third-party cookies without a CP
 - Rejects unsatisfactory third-party cookies




No P3P syntax checking in IE

- IE accepts P3P policies containing bogus tokens or missing required tokens
- Example of valid compact policy:

 **CAO DSP COR CURa ADMa DEVa OUR
IND PHY ONL UNI COM NAV INT DEM PRE**

- Examples of invalid policies accepted by IE:

 **AMZN**

 **Facebook does not have a P3P policy.
Learn why here: <http://fb.me/p3p>**

P. Leon, L. Cranor, A. McDonald, and R. McGuire. Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens. WPES 2010.

[MSDN Blogs](#) > [IEBlog](#) > [Google Bypassing User Privacy Settings](#)

Google Bypassing User Privacy Settings

Published Monday, February 20, 2012 1:31 PM

 152 comments

When the IE team heard that Google had bypassed user privacy settings on Safari, we asked ourselves a simple question: is Google circumventing the privacy preferences of Internet Explorer users too? We've discovered the answer is yes: Google is employing similar methods to get around the default privacy

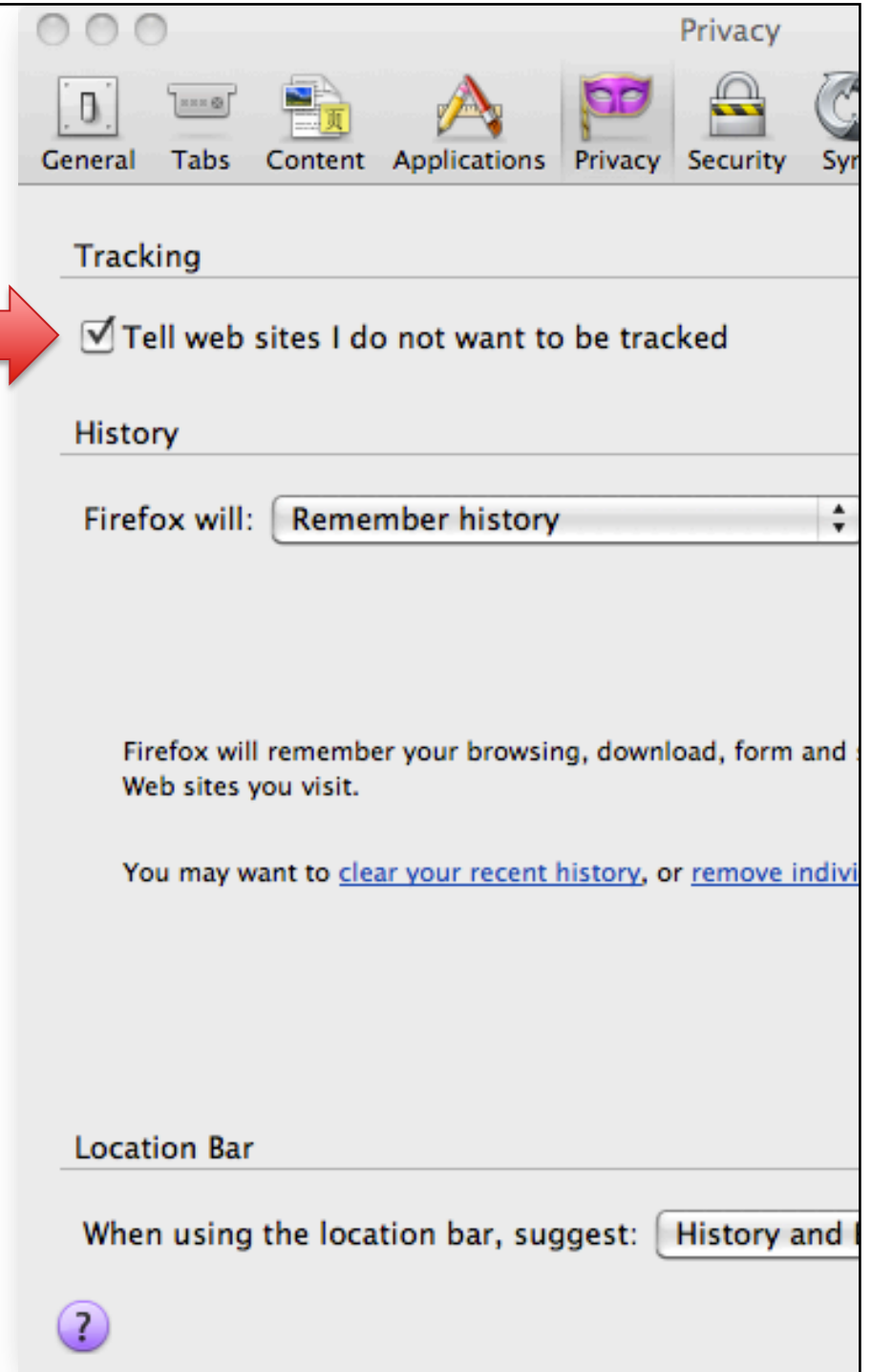
Languages

[English](#)[Français](#)[Deutsch](#)[Português \(Brasil\)](#)[한국어](#)[日本語](#)[简体中文](#)[Русский](#)

Microsoft uses a “self-declaration” protocol (known as “P3P”) dating from 2002 It is well known – including by Microsoft – that it is impractical to comply with Microsoft’s request while providing modern web functionality.

Do not track

- Proposed W3C standard
- User checks a box
- Browser sends “do not track” header to website
- Website stops “tracking”
- W3C working group trying to define what that means



Lots of tools to stop tracking

- Browser privacy settings
 - Cookie blocking
 - P3P
 - Tracking Protection Lists
 - Do Not Track
- Browser add-ons
- Opt-out cookies
- Digital Advertising Alliance (DAA) AdChoices icon and associated opt-out pages



Are any of these tools effective?

- Do the tools work?
 - Does technology do what it is supposed to do?
 - Do companies respect user choices?
- Can consumers use them?
 - Do users understand tracking?
 - Do users understand what tools do?
 - Can users make tools do what they want?

Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising

Pedro G. Leon, Blase Ur, Rebecca
Balebako, Lorrie Faith Cranor,
Richard Shay, and Yang Wang
CHI 2012

Three types of tools tested

Blocking Tools



Opt-out Tools



Privacy built in browser



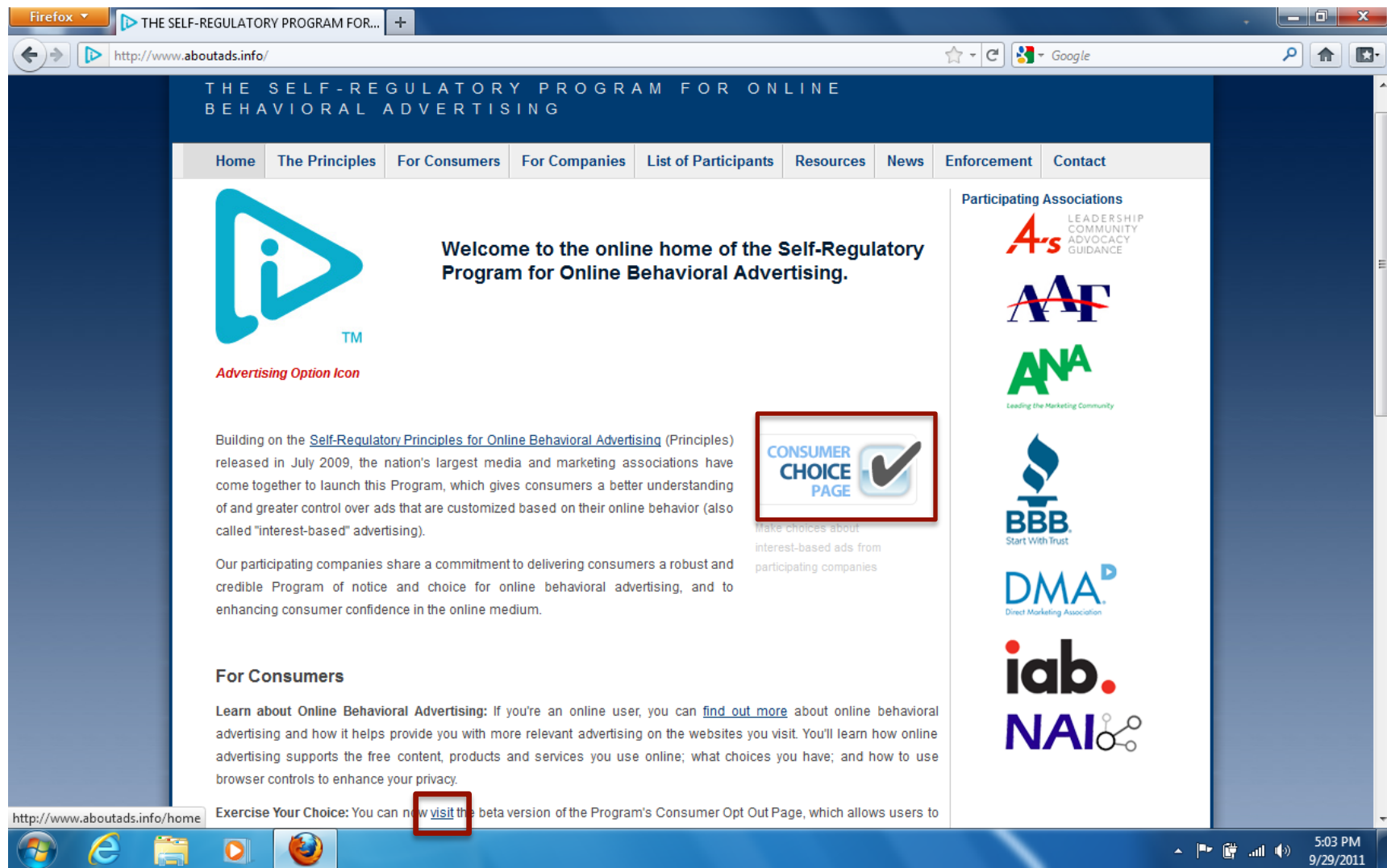
Methodology

- Part of previous interview study
- 45 participants evaluated 9 tools
 - Between subjects study
 - Random assignment, controlled for preferred web browser and operating system

Testing protocol

- Semi-structured interview
- Usability testing
 - Task 1: Learn about and install the tool
 - Task 2: Change tool settings
 - Task 3: Browsing scenarios
- Exit questionnaire

DAA website



Opting out can be challenging



Translate

From: Japanese - detected ▼



To: English ▼

Translate

すでにターゲティング広告が配信されている場合、すべての配信停止処理にはお時間かかる場合があります。
この処理は、ユーザー情報を参考にしたターゲティング広告を配信停止しただけになっていますので、それ以外の広告配信については停止処理を行っていませんこと、ご了承下さい。

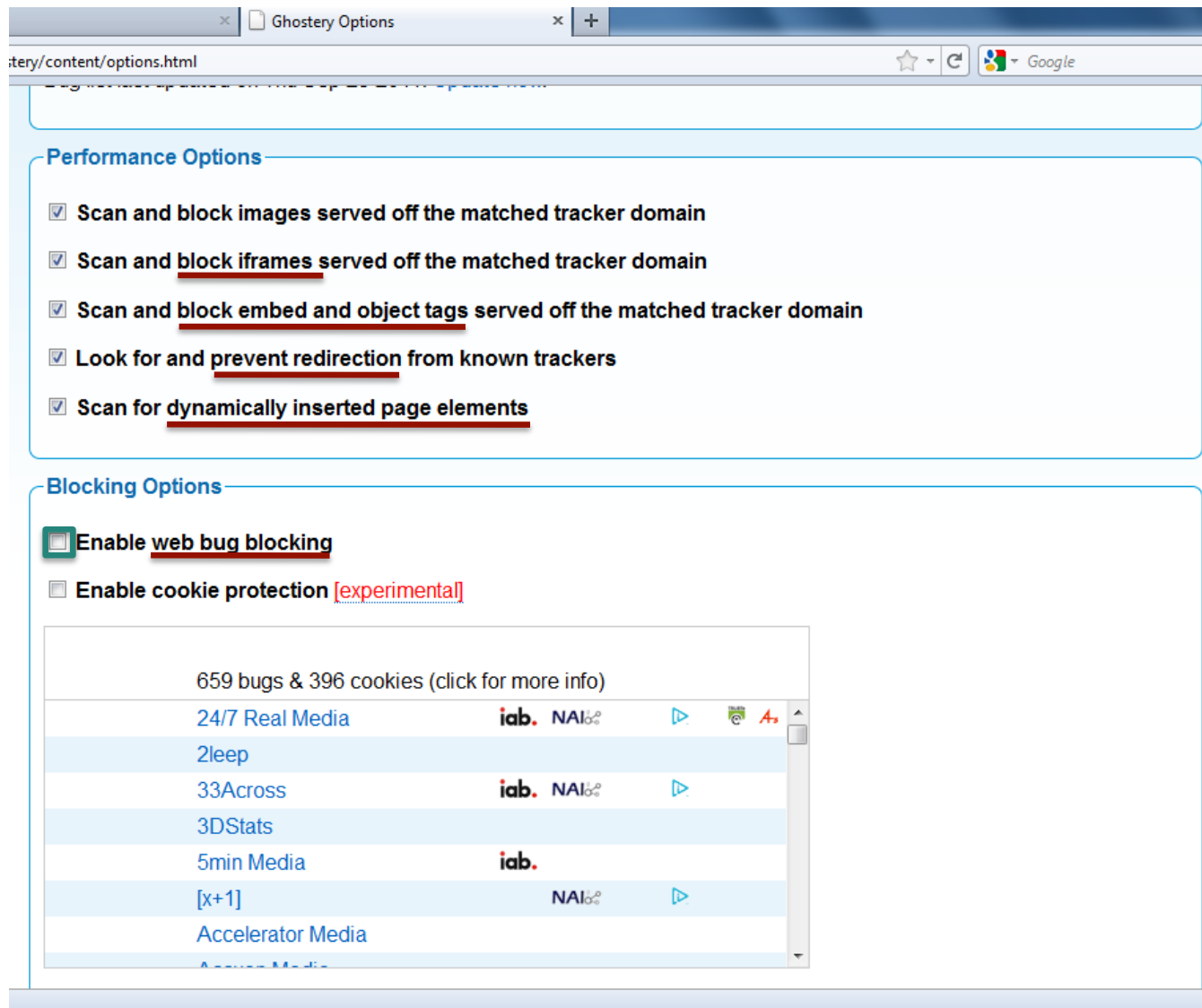
Ä

If you have already targeted ads are delivered, all unsubscribe process may take your time.
This process has not only stop targeting ads that reference the user information for ad serving, otherwise it does not stop in the process, please understand.

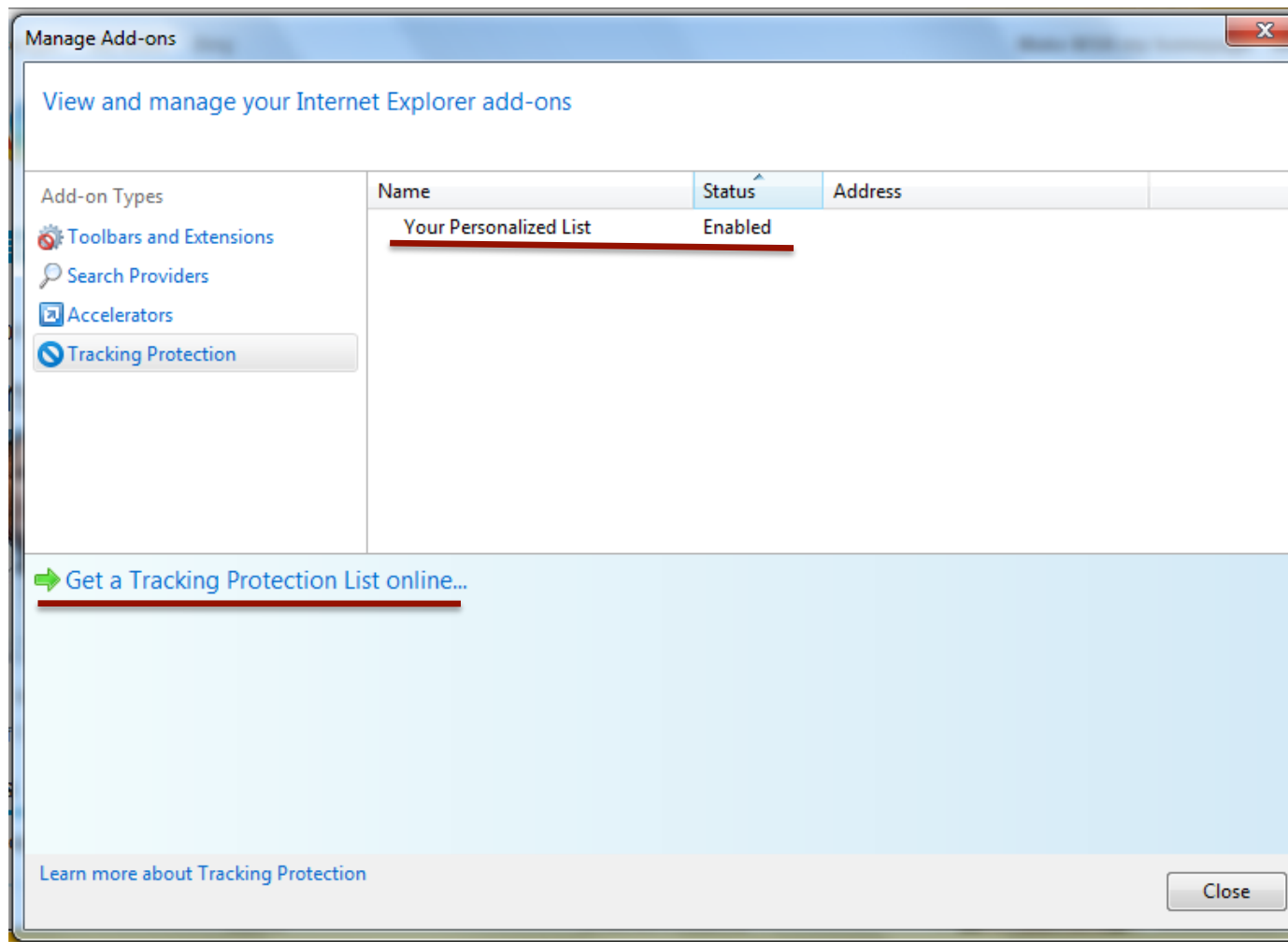


New! Click the words above to view alternate translations. [Dismiss](#)

Ghostery configuration interface



IE-TPL configuration interface



Takeaways

- Problematic defaults
- Poorly designed interfaces and jargon
- Feedback
- Misconceptions about opt-out tools
- Users unable to make meaningful decisions on a per-company basis

What Do Online Behavioral Advertising Disclosures Communicate to Users?

Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. WPES 2012



AdChoices



Pop in. Stand out.

Buy Now!

TARGET P&G eStore amazon.com

AT&T.

The nation's
largest
4G
network.



LEARN MORE

Rethink Possible®

4G speeds not available everywhere.

It's 1702, a decade after
The Crucible's infamous seductress
danced with the devil in Salem.

MAY 4-26, 2013

Abigail
1702

BY ROBERTO AGUIRRE-SACASA
DIRECTED BY TRACY BRIGDEN

CITY THEATRE

BUY TICKETS >

YAHOO!
--- ON THE ---
ROAD

Don't miss a beat

Ad Feedback

AdChoices

The industry claims total success

“The DAA has revolutionized consumer education and choice by delivering a real-time, in-ad notice more than 10 billion times every day through the increasingly ubiquitous DAA Advertising Option Icon (also known as the ‘Ad Choices’ Icon)”



Peter Kosmala, Former Managing Director of The Digital Advertising Alliance. *Yes, Johnny Can Benefit From Transparency and Control.* November 3, 2011.

Objectives

- Evaluate the effectiveness of different OBA disclosures at communicating notice and choice about OBA
- Find ways to improve effectiveness of OBA disclosures

Methodology

- Large scale between-subjects online study
 - 1,505 participants
 - Over 100 participants per treatment
- Participants recruited through Amazon Mechanical Turk
- Guided browsing scenario
- Online survey

First exposure to OBA disclosures

HOME PAGE TODAY'S PAPER VIDEO MOST POPULAR TIMES TOPICS

Subscribe: Home Delivery / Digital Log In Register Now

Why did I get this ad? 

The New York Times

Tuesday, October 25, 2011 Last Update: 11:21 PM ET

CLICK HERE

Follow Us    Subscribe to Home Delivery Personalize Your Weather

Switch to Global Edition ▶

JOBS
REAL ESTATE
AUTOS
ALL CLASSIFIEDS

WORLD
U.S.
POLITICS
NEW YORK
BUSINESS
DEALBOOK
TECHNOLOGY
SPORTS
SCIENCE
HEALTH
OPINION
ARTS
Books
Movies
Music
Television
Theater
STYLE
Dining & Wine
Fashion & Style
Home & Garden
Weddings/

Europe Faces New Hurdles in Crisis Over Debt

By STEVEN ERLANGER and RACHEL DONADIO 20 minutes ago

On the eve of a European Union summit meeting, crucial financial measures were still unresolved.

- Tempers Flare as European Meeting Nears

I.B.M. Names Virginia Rometty as New Chief Executive

By STEVE LOHR 22 minutes ago

The selection of Ms. Rometty, a senior vice president at I.B.M., will make her one of the highest-profile women executives in corporate America.



Baseball's Game of Telephone

By PAT BORZI 3 minutes ago

Monday night's bullpen debacle by the Cardinals has put a new spotlight on baseball's reliance on landlines.

New Poll Finds a Deep Distrust of Government

By JEFF ZELENY and MEGAN THEE-BRENAN 3 minutes ago

With Election Day just over a year away, a deep

OPINION »

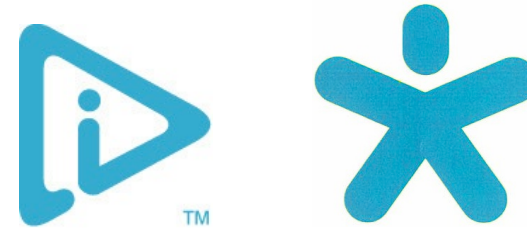
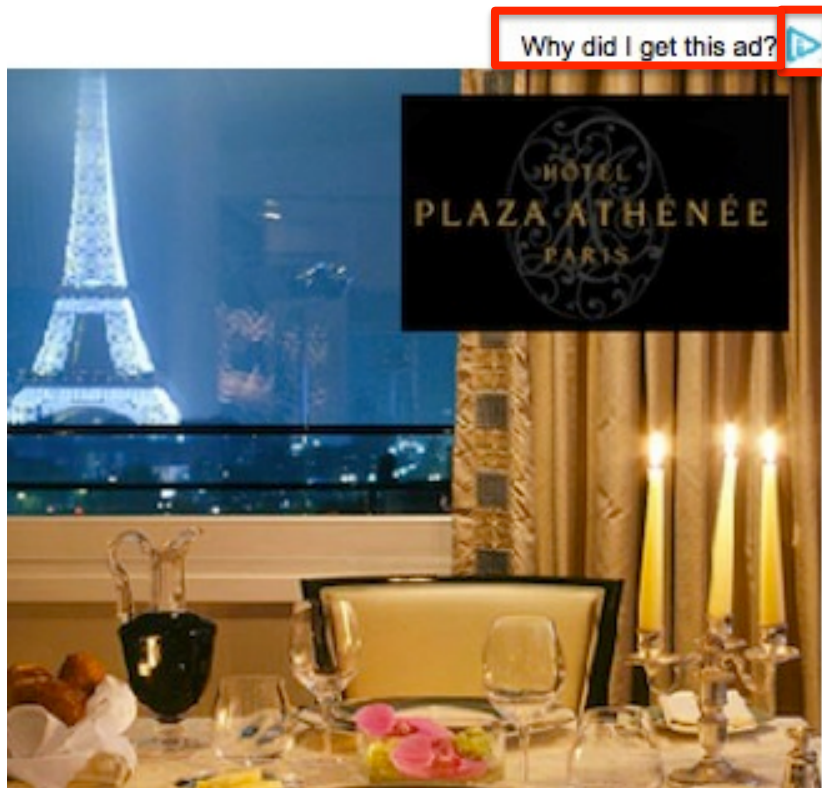
OP-ED | CLIFFORD WINSTON
Are Law Schools and Bar Exams Necessary?
The barriers to entry for the legal industry exist to protect lawyers from competition with non-lawyers.

- Brooks: The Fighter Fallacy | Comments
- Nocera: Jobs's Biographer
- Cohen: Defending the E.U.
- Bruni: Have Glock
- Editorial: Refinancing
- Room for Debate: Will Amazon Kill Off Publishers?

Why did I get this ad? 



Second exposure to OBA disclosures



- Why did I get this ad?
- Interest based ads
- AdChoices
- Sponsor ads
- Learn about your ad choices
- Configure ad preferences
- 'No tagline'

Exposure to landing pages

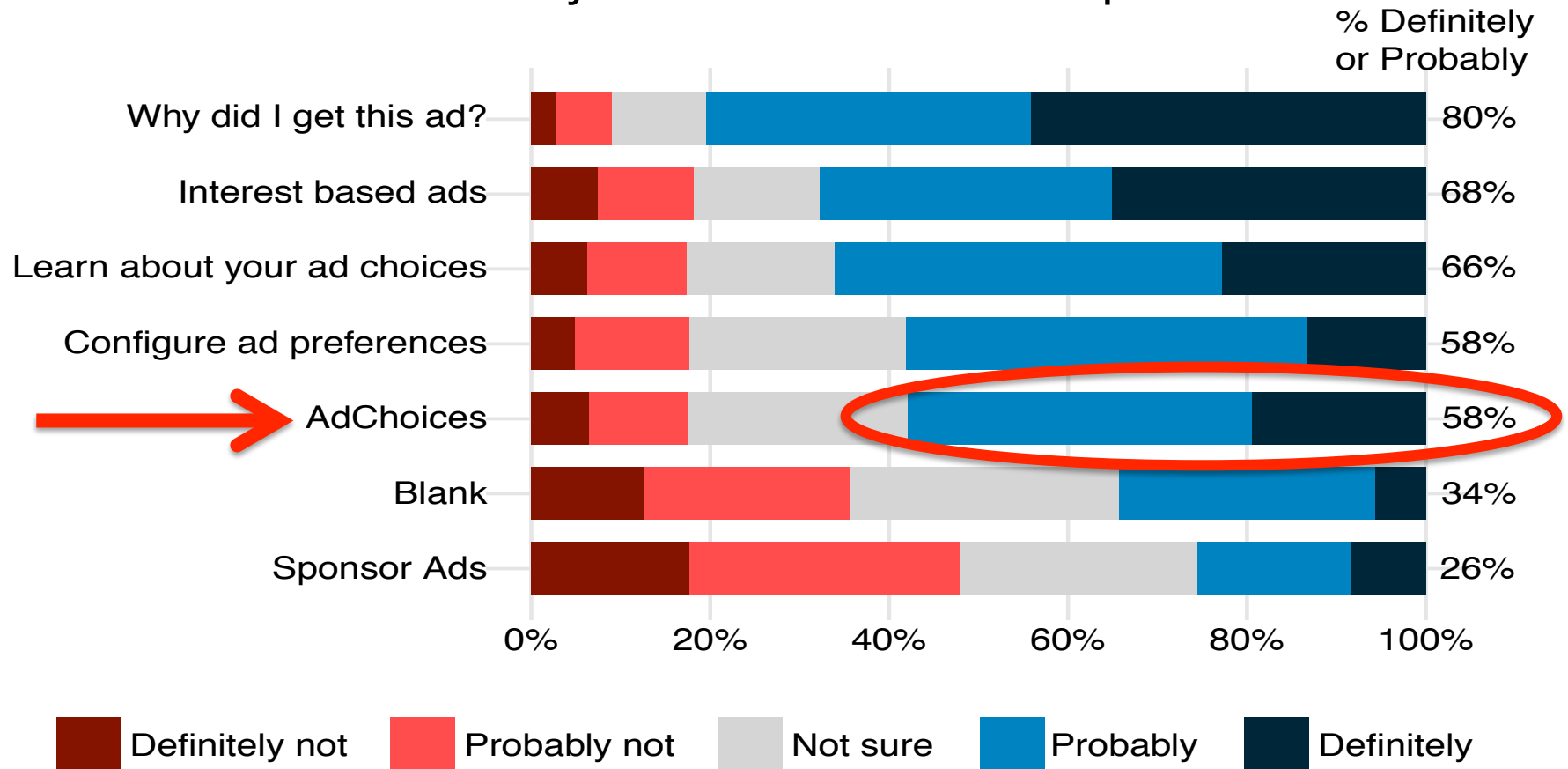


- AOL
- Yahoo!
- Microsoft
- Google
- Monster

Do icons and taglines suggest tailored ads?

- To what extent, if any, does this combination of the symbol and phrase, placed on the top right corner of the above ad suggest the following?
 - This ad has been tailored based on websites you have visited in the past. [true]

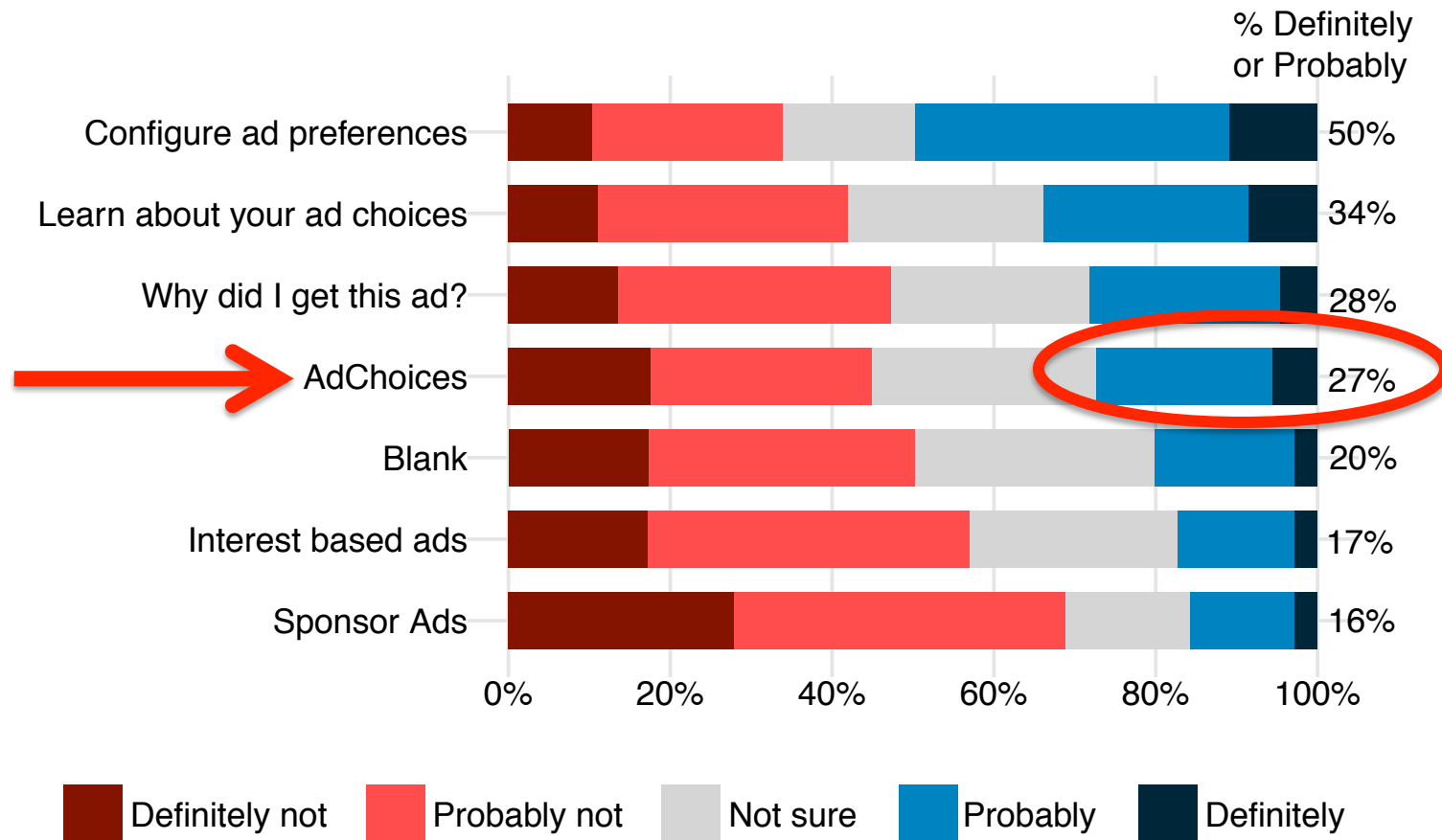
This ad has been tailored based on websites you have visited in the past



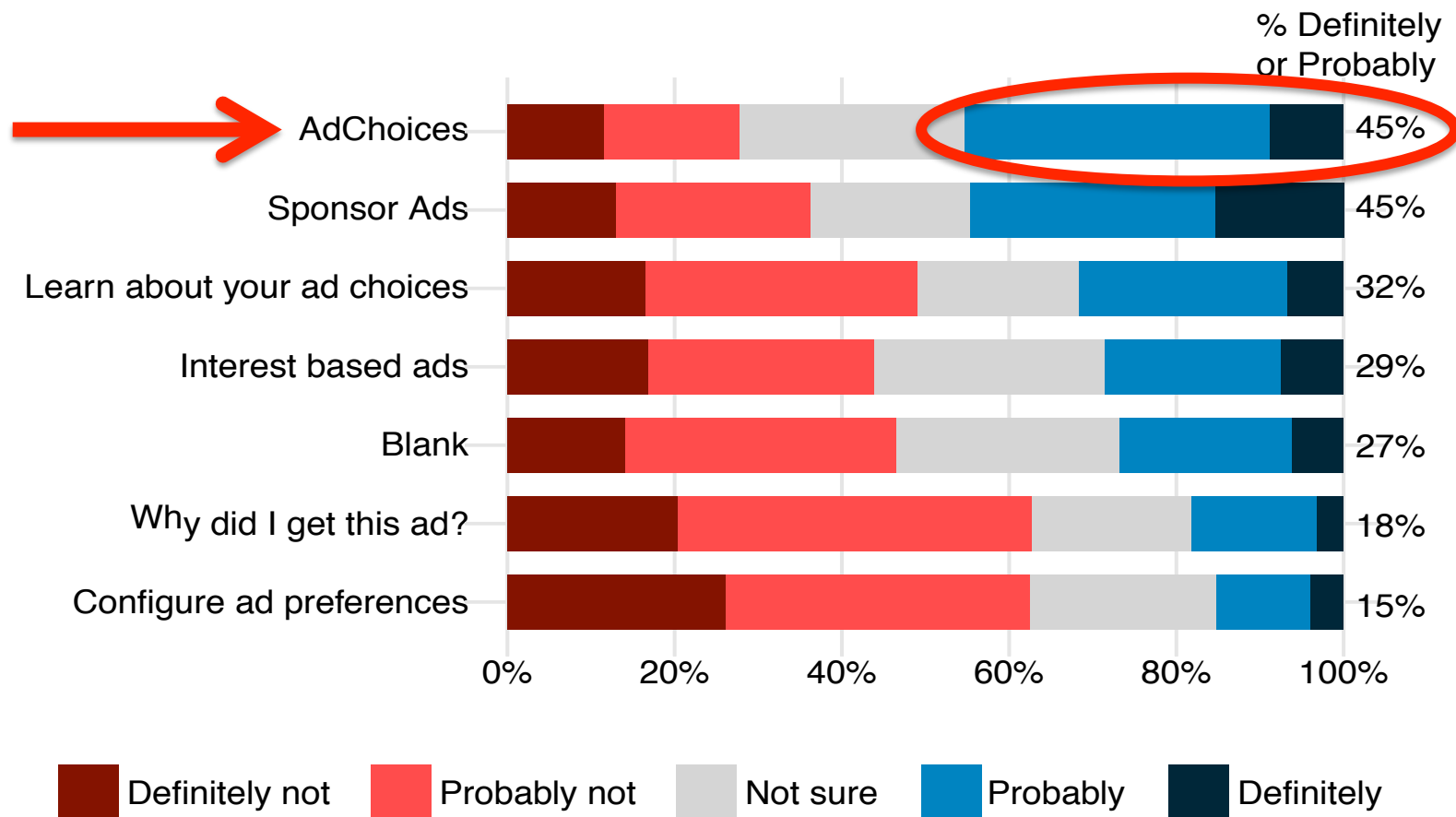
Willingness to click

- What do you think would happen if you click on that symbol or that phrase?
 - It will take you to a page where you can tell the advertising company that you do not want to receive tailored ads. [true]
 - More ads will pop up. [false]
 - It will take you to a page where you can buy advertisements on this website. [false]

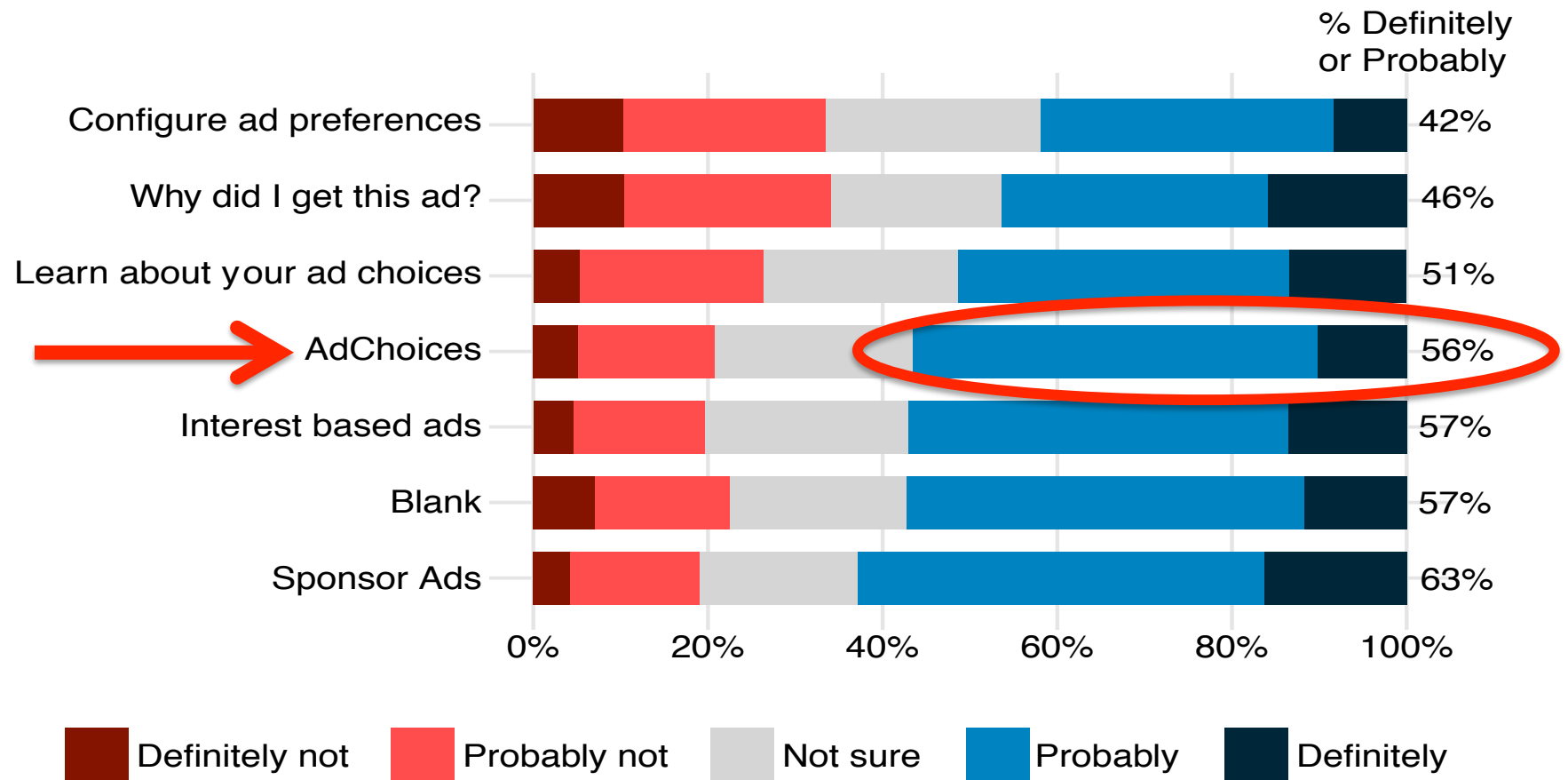
Will take you to a page where you can tell the advertising company that you do not want to receive tailored ads



Will take you to a page where you can
buy advertisements on this website



More ads will pop up



Takeaways

- OBA icons and taglines are not noticed
- “AdChoices” was outperformed by other tagline treatments at communicating notice and choice about OBA
- Users are afraid to click on icon

How effective is privacy
notice and choice in practice?

Notice and Choice Mechanism	Effectiveness in Practice
Privacy policies	
Privacy nutrition labels	
Privacy Facts for Android	
P3P	
Do Not Track	
Tools to opt-out of tracking	
AdChoices icon	
Model financial privacy notice	

Notice and Choice Mechanism	Effectiveness in Practice
Privacy policies	Nobody reads
Privacy nutrition labels	Promising research, not used
Privacy Facts for Android	Promising research, not used
P3P	Used to circumvent browser privacy settings
Do Not Track	No agreement on what it means
Tools to opt-out of tracking	Difficult to use
AdChoices icon	Nobody knows what it means and people are afraid to click on it
Model financial privacy notice	Adopted by thousands of websites, could be more useful with directory

How to make notice and choice more effective

- Incentives for adoption
- Enforcement (legal and technical)
- Baseline requirements
- Standardized notice formats
- Machine-readable notice formats
- Reduce ambiguity
- Link to full disclosure
- Comparison tools
- More research

Are They Actually Any Different? Comparing Thousands of Financial Institutions' Privacy Practices

Lorrie Faith Cranor, Kelly Idouchi,
Pedro Giovanni Leon, Manya
Sleeper, Blase Ur, WEIS 2013



Rev. June 2012

FACTS	WHAT DOES PNC DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: <ul style="list-style-type: none">▪ Social Security number and income▪ Account balances and account transactions▪ Credit scores and payment history
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information, the reasons PNC chooses to share, and whether you can limit this sharing.

Reasons we can share your personal information	Does PNC share?	Can you limit this sharing?
For our everyday business purposes — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes — to offer our products and services to you	Yes	No
For joint marketing with other financial companies	Yes	Yes
For our affiliates' everyday business purposes — information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes — information about your creditworthiness	Yes	Yes
For our affiliates to market to you	Yes	Yes
For nonaffiliates to market to you	No	We don't share

To limit our sharing	<ul style="list-style-type: none">▪ Call 1-800-762-2118 — our menu will prompt you through your choice(s)▪ Visit us online: www.PNC.com/privacy (Online Banking customers only.) <p>Please note: If you are a <i>new</i> customer, we can begin sharing your information 30 days from the date we sent this notice. When you are <i>no longer</i> our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.</p>
Questions?	Call 1-800-762-2118

160787-0312

IC#00085294

3.NF-082-SI-0612
0030T6

FACTS	WHAT DOES CIT Group Inc. ("CIT") DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depends on the product or service you have with us. This information can include: <ul style="list-style-type: none"> • Social Security Number and income • account balances and transaction history • credit history and credit scores When you are no longer our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons CIT chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information

	Does CIT share?	Can you limit this sharing?
For our everyday business purposes — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes — to offer our products and services to you	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes — information about your transaction	No	We don't share
For our affiliates' everyday business purposes — information about your creditworthiness	Yes	No
For nonaffiliates to market to you	No	No

Questions? Call: 1-800-687-
policy/index.h

FACTS	WHAT DOES BANK OF AMERICA DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Under federal law, that means personally identifiable information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: <ul style="list-style-type: none"> • Social Security number and employment information • account balances, transaction history and credit information • assets and investment experience All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Bank of America chooses to share; and whether you can limit this sharing.
How?	

Reasons we can share your personal information

	Does Bank of America share?	Can you limit this sharing?
For our everyday business purposes — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes — with service providers we use to offer our products and services to you (Please see below to limit the ways we contact you)	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes — information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes — information about your creditworthiness	Yes	Yes
For nonaffiliates to market to you — for all credit card accounts	Yes	Yes
For nonaffiliates to market to you — for accounts and services endorsed by another organization (e.g., debit card co-branded with a baseball team) "Sponsored Accounts"	Yes	Yes
For nonaffiliates to market to you — for accounts other than credit card accounts and Sponsored Accounts, such as insurance, investments, deposit and lending	No	We don't share

55

Gramm-Leach Bliley Act (1999)

- Mandated annual privacy disclosures
- Disclosures were full of fine print, difficult to read and compare



Standardized notice

- Eight federal agencies jointly released a model privacy form (2009)
 - Two pages
 - Optional, but widely adopted
 - Safe harbor

Model Privacy Form

Rev. (insert date)

FACTS

WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.	
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: <ul style="list-style-type: none">■ Social Security number and [income]■ [account balances] and [payment history]■ [credit history] and [credit scores]	
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.	
Reasons we can share your personal information	Does [name of financial institution] share?	Can you limit this sharing?
For our everyday business purposes—such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes—to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes—information about your transactions and experiences		
For our affiliates' everyday business purposes—information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		
To limit our sharing	<ul style="list-style-type: none">■ Call [phone number]—our menu will prompt you through your choice(s)■ Visit us online: [website] or■ Mail the form below <p>Please note:</p> <p>If you are a new customer, we can begin sharing your information [30] days from the date we sent this notice. When you are no longer our customer, we continue to share your information as described in this notice.</p> <p>However, you can contact us at any time to limit our sharing.</p>	
Questions?	Call [phone number] or go to [website]	

Mail-in Form

Leave Blank OR (If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.) <input type="checkbox"/> Apply my choices only to me	Mark any/all you want to limit: <ul style="list-style-type: none"><input type="checkbox"/> Do not share information about my creditworthiness with your affiliates for their everyday business purposes.<input type="checkbox"/> Do not allow your affiliates to use my personal information to market to me.<input type="checkbox"/> Do not share my personal information with nonaffiliates to market their products and services to me.
Name	Mail to:
Address	[Name of Financial Institution]
City, State, Zip	[Address1]
[Account #]	[Address2]
	[City], [ST] [ZIP]

Page 2

Who we are

Who is providing this notice?

[insert]

What we do

How does [name of financial institution] protect my personal information?

To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.

[insert]

How does [name of financial institution] collect my personal information?

We collect your personal information, for example, when you

- [open an account] or [deposit money]
- [pay your bills] or [apply for a loan]
- [use your credit or debit card]

[We also collect your personal information from other companies.]

OR

[We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]

Why can't I limit all sharing?

Federal law gives you the right to limit only

- sharing for affiliates' everyday business purposes—information about your creditworthiness
- affiliates from using your information to market to you
- sharing for nonaffiliates to market to you

State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]

What happens when I limit sharing for an account I hold jointly with someone else?

[Your choices will apply to everyone on your account.]

OR

[Your choices will apply to everyone on your account—unless you tell us otherwise.]

Definitions

Affiliates

Companies related by common ownership or control. They can be financial and nonfinancial companies.

- [affiliate information]

Nonaffiliates

Companies not related by common ownership or control. They can be financial and nonfinancial companies.

- [nonaffiliate information]

Joint marketing

A formal agreement between nonaffiliated financial companies that together market financial products or services to you.

- [joint marketing information]

Other important information

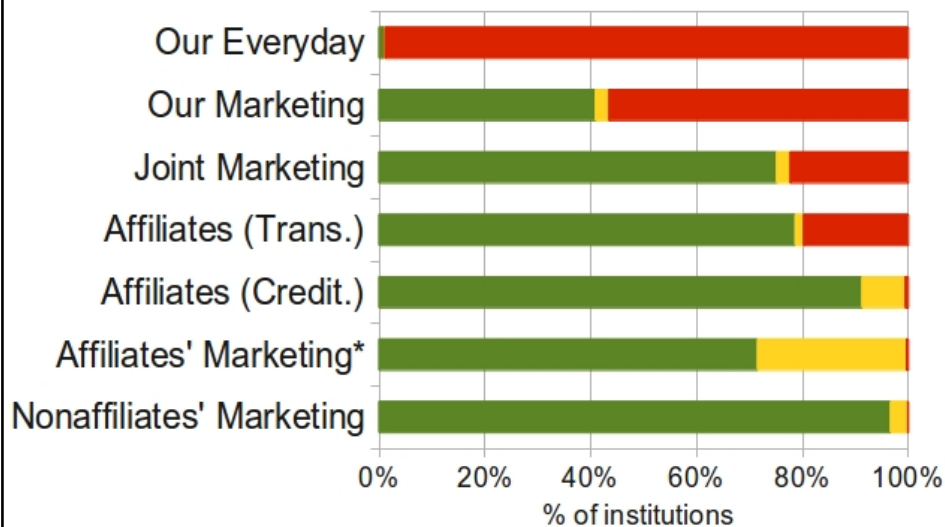
[insert other important information]

Data collection and extraction

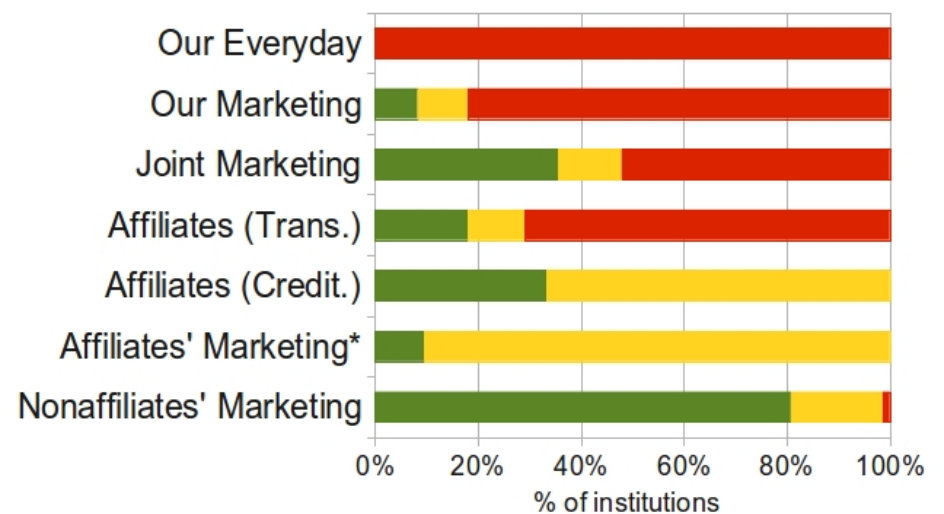
- FDIC directory of 7,072 institutions
- Searched for them all with Google queries
- Found model privacy form in HTML or PDF
- Parsed form and put it in a database
 - Many errors and deviations from model form had to be accounted for
 - Manual check shows our parsing accuracy to be >90%
- Currently collecting data for larger list FOIAed from the Federal Reserve

Sharing practices

Entire sample



100 largest banks



■ Don't share

■ Share, opt-out

■ Share, no opt-out

What Info is Collected, and How

- What: 24 options, SSN + choose exactly 5

What?

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and [income]
- [account balances] and [payment history]
- [credit history] and [credit scores]

- How: 34 options, choose exactly 5

How does [name of financial institution] collect my personal information?

We collect your personal information, for example, when you

- [open an account] or [deposit money]
- [pay your bills] or [apply for a loan]
- [use your credit or debit card]

- The most commonly used terms were the examples listed in the model

Curiosities Encountered

- Self-contradictory statements (15)

Does Geneva State
Bank share?

Yes

Yes

Yes

Curiosities Encountered

- Self-contradictory statements (15)

Does Geneva State Bank share?	Can you limit this sharing?
Yes	We don't share
Yes	We don't share
Yes	We don't share

Curiosities Encountered

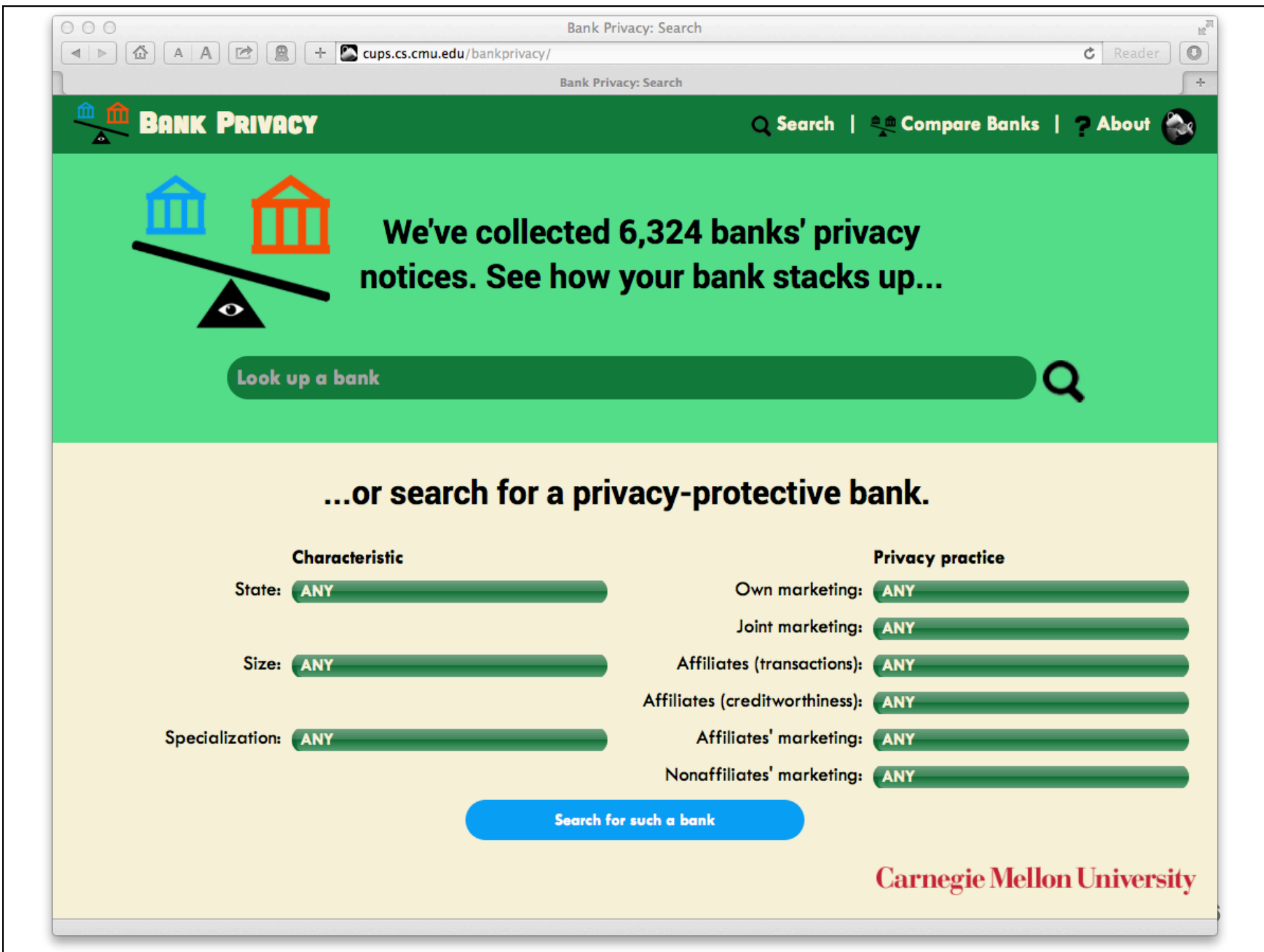
- Self-contradictory statements (15)

Does Geneva State Bank share?	Can you limit this sharing?
Yes	We don't share
Yes	We don't share
Yes	We don't share

- 24 institutions appear to be violating the Fair Credit Reporting Act (FCRA)
 - Not providing required opt-outs

Takeaways

- Model form needs some improvement
- Adoption happens when there are incentives
- Institutions are actually different!
 - Largest institutions have the worst practices
 - Opportunity for consumer privacy choice
- But we need to help consumers find the banks with good privacy





Carnegie Mellon University
CyLab

isr institute for
SOFTWARE
RESEARCH

Engineering &
Public Policy